Remarks

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1-10, and 22 are currently pending;
- Claims 11-21 are withdrawn; and
- Claims 1 and 9 are amended herein.

[0003] Support for the amendments to claims 1 and 9 are found in the specification at least at paragraph 20 of page 1; and paragraph 10 of page 12.

Cited Documents

[0004] The following documents have been applied to reject one or more claims of the application:

- Fisher: Addison M. Fisher, U.S. Patent No. 6,141,423 (Fisher);
- Kao: I-Lung Kao, U.S. Patent No. 7,451,147 B1 (Kao);
- Ault: Michael Bradford Ault, U.S. Patent No. 5,918,228 (Ault); and
- Patel: Paresh Patel, U.S. Patent No. 6,438,690 (Patel).

Overview of the Application

[0005] The Application relates to a secured distributed impersonation, such as can be used within batch systems (e.g., batch message transaction systems). In one embodiment, a method includes sending a request for network account credentials from an originating account associated with an unpublished object, to a dispatch associated with a published object. In one embodiment, both the unpublished and the published objects can each be a message queue. The request is sent specifically to the published object, and identifies the unpublished object. The originating account can be at a local computer, for example, within a system of which the dispatch is also a part. The network account credentials can be, for example, the account credentials that the originating account needs to properly perform a job that has been assigned to it.

[0006] The dispatch authenticates the originating account. Upon successful authentication, the network account credentials are sent to the originating account. In one embodiment, these account credentials are included in data that is generically referred to as non-restrictive and non-limited emblem. The emblem in one embodiment can be a secure manner by which the credentials are transmitted. For example, the emblem can be a token, as known within the art. The emblem is specifically sent to the unpublished object associated within the originating account, as identified in the initial request. The network account for which the originating account requested credentials can be a batch account of the dispatch itself, in one embodiment, while in another embodiment it can be an agent account onto which the dispatch proxy logs. In either case, the dispatch has the network account remoted back to the originating account. Furthermore, the network account can be any of a number of agent accounts, such that

any of the agent accounts may be remoted back to the originating account as the network account. Thus, the request for a network account may be a request for the credentials of a particular agent account, or for the credentials of any of a group of agent accounts.

Overview of Fisher

[0007] Fischer describes a method of reducing an inadvertent betrayal towards an owner of escrowed digital secrets by a trustee. The escrowed digital secrets are encrypted for security measures, and may include the owner's identification information. The escrowed digital secrets may also include secret information (e.g., Swiss bank account information) that could potentially harm the owner if an imposter were to obtain the secret information. In a case where the owner misplaces a private key to the escrowed digital secrets, the owner may contact the trustee with an encrypted request to view the escrowed digital secrets. The owner may also be given the private key to decrypt and view the escrowed digital secrets. To make sure that the owner is not an imposter, the trustee may require certain credentials that will identify the owner (e.g., the identification information contained within the escrowed digital secrets). If the credentials are not sufficient, then the alleged owner may be treated as an imposter and be denied of the initial request. In an embodiment, the trustee may require additional credentials. If the credentials are sufficient, then the escrowed digital information or the private key may be granted to the proven owner.

Overview of Kao

[0008] Kao describes a method in a data processing system for providing security to target passwords in a global sign on system centralized database. In a preferred

embodiment, a target password is received by the global sign on system. The target password is encrypted in a user selected encryption manner to create an encrypted password. The encrypted password and an indication of encryption manner chosen is then stored in the centralized database.

Based on the cited case of Fisher in view of Kao, Ault, and Patel, claims 1-10, and 22 are rejected under 35 U.S.C. 103(a).

Claims 1-10, and 22 are Patentable Over Fisher in view of Kao, Ault, and Patel.

[0009] Claims 1-10, and 22 stand rejected under 35 U.S.C. § 103(*a*) as allegedly being anticipated by Fisher in view of Kao, Ault, and Patel. Applicant respectfully traverses the rejection.

Independent Claim 1

[0010] Applicant submits that Fisher in view of Kao does not teach Claim 1, because the references do not disclose, at least, the following features of Claim 1, as amended (with emphasis added):

> sending a request for network account credentials from an **originating account to complete an assigned job**, at a dispatch associated with a published object, the request directed to the published object associated with the dispatch includes identification of an unpublished object associated with the originating account.

[0011] In rejecting Claim 1, the Office cites Fisher (Col. 10, lines 14-42) in view of Kao (Col. 3, lines 33-50). Col. 10, lines 14-42 of Fisher states that "it is contemplated that a public key may be required from the applicant to define the public key under which the applicant wants the information returned. In this fashion, the trustee and the applicant may secretly communicate without any danger of the secret information being revealed to an opponent who intercepts the communication." Col. 3, lines 33-50 of Kao further states "when a user of a client, such as one of clients 108, 110 or 112, requests a service, an application, or information from a database from a target, which requires a password to access, a request for the appropriate user password is sent to GSO server 120. GSO server 120 retrieves the appropriate information from GSO target information database 124, decrypts the password (if the password has been encrypted), and passes the unencrypted password back to the requesting client. The requesting client then sends the request along with the password to the target to access a service, application or database. In this way, a user of network 100 is only required to remember one password in order to log on to network 100. If any passwords or user information is required by an application, service, or database, those passwords are stored in GSO target information database 124 in encrypted form until use of one of the target passwords is needed."

[0012] Fisher teaches an applicant (i.e., escrow information owner) sending the public key to define the public key under which the applicant wants the information returned; however, the claim recites "sending a request for network account credentials from an originating account to complete an assigned job, at a dispatch associated with a published object,..." As shown, Fisher teaches that the applicant (i.e., escrow

information owner) who retrieves the information from an escrowed account, without using the information to complete the assigned job (e.g., processing a transaction). Accordingly, the cited portions of Fisher do not teach or suggest the "originating account to complete an assigned job" as recited in Claim 1.

[0013] Kao teaches a user logging on to a network using a single password, and a requesting client sending a request to a target to access a service, application or database; however, the claim recites "an originating account to complete an assigned job,…." Kao teaches a process of logging onto the network through the single password and be able to access other network accounts requiring different passwords. Kao does not teach the user or the requesting client to complete the assigned job. For example, the Application describes the originating account to execute an assigned batch job (e.g., processing of transactions during non-peak periods). As such, Kao teaches the logging on process (i.e., through the single password) which is different from completing the assigned job (e.g., batch job).

[0014] Consequently, Fisher in view of Kao does not teach or suggest all of the elements and features of Claim 1. Accordingly, Applicant respectfully requests that the rejection of Claim 1 be withdrawn.

Dependent Claims 2-8, and 22

[0015] Claims 2-8, and 22 ultimately depend from independent Claim 1. As discussed above, Claim 1 is allowable. Therefore, Claims 2-8, and 22 also stand allowable for at least their dependency from an allowable base Claim 1.

Independent Claim 9

[0016] Applicant submits that Fisher in view of Kao does not disclose Claim 9, because Fisher does not disclose, at least, the following features of Claim 9, as amended (with emphasis added):

> The method of claim 1, wherein sending an emblem for the network account to the originating account comprises:
>
> proxy logging on to the agent; and
>
> remoting an agent account to the **originating account to complete an assigned job** upon proxy log on to the agent, such that the emblem comprises an emblem for the agent account.

[0017] In rejecting Claim 9, the Office Action cites the same reasons for rejecting Claim 1. The Applicant respectfully traverses the rejection on this ground.

[0018] The Applicant respectfully provides arguments in support of Claim 9 as discussed in support of Claim 1 above.

[0019] Consequently, Fisher in view of Kao does not teach or suggest all of the elements and features of Claim 9. Accordingly, Applicant respectfully requests that the rejection of Claim 9 be withdrawn.

Dependent Claim 10

[0020] Claim 10 ultimately depend from independent Claim 9. As discussed above, Claim 9 is allowable. Therefore, Claim 10 also stands allowable for at least its dependency from an allowable base Claim 9.

[0021] Consequently, Fisher in view of Kao does not disclose all of the elements and features of Claim 10. Accordingly, Applicant respectfully requests that the rejection of Claim 10 be withdrawn.

Conclusion

[0022] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned representative for the Applicant before issuing a subsequent Action.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/Emmanuel A. Rivera/ Dated: May 14, 2009

Emmanuel A. Rivera (Emmanuel@leehayes.com; 512-505 8162, ext 5001)
Registration No. 45,760

Telephone: (512) 505-8162
Facsimile: (509) 323-8979
www.leehayes.com